(12) UK Patent Application (19) GB (11) 2 303 173 (13) A

(43) Date of A Publication 12.02.1997

(21) Application No 9614616.2

(22) Date of Filing 11.07.1996

(30) Priority Data
(31) 9514096 (32) 11.07.1995 (33) GB

(71) Applicant(s)
Clive Robert Homewood
16 The Crescent, STANFORD, Beds, SG18 9JF, United Kingdom

Steve Croft
27 Ashwell Close, Graveley, HITCHIN, Herts, SG4 7LH, United Kingdom

(72) Inventor(s)
Clive Robert Homewood
Steve Croft

(74) Agent and/or Address for Service
Britter & Co
Barn West, The Dixies, High Street, Ashwell, BALDOCK, Hertfordshire, SG7 5NT, United Kingdom

(51) INT CL^6
G08B 15/02

(52) UK CL (Edition O)
E2X X8

(56) Documents Cited
GB 2280056 A GB 2269205 A EP 0347091 A
EP 0196944 A1 WO 80/00887 A US 4908608 A

(58) Field of Search
UK CL (Edition O) E2X
INT CL^6 E05G 1/14 , G08B 15/02
On-line: WPI

(54) Computer Security Module

(57) A security device for electrical or electronic equipment (eg a computer) comprises a sealed unit of dye with rupture lines (9), rechargeable batteries (6), an audible alarm (10), a gas cartridge (7), a gas motor (8), and an electronics module (5). Within the electronics module (5) a plurality of monitoring means are housed which can detect a deviation from normal use of the protected equipment and thus initiate sounding of the alarm and release of the dye over the components of the equipment. The monitoring means may include light, motion and spatial detectors.

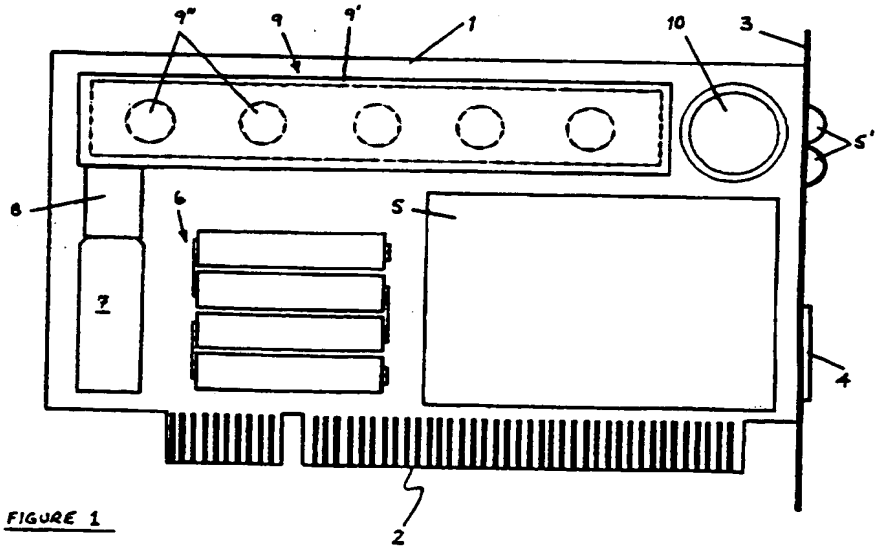

FIGURE 1

GB 2 303 173 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

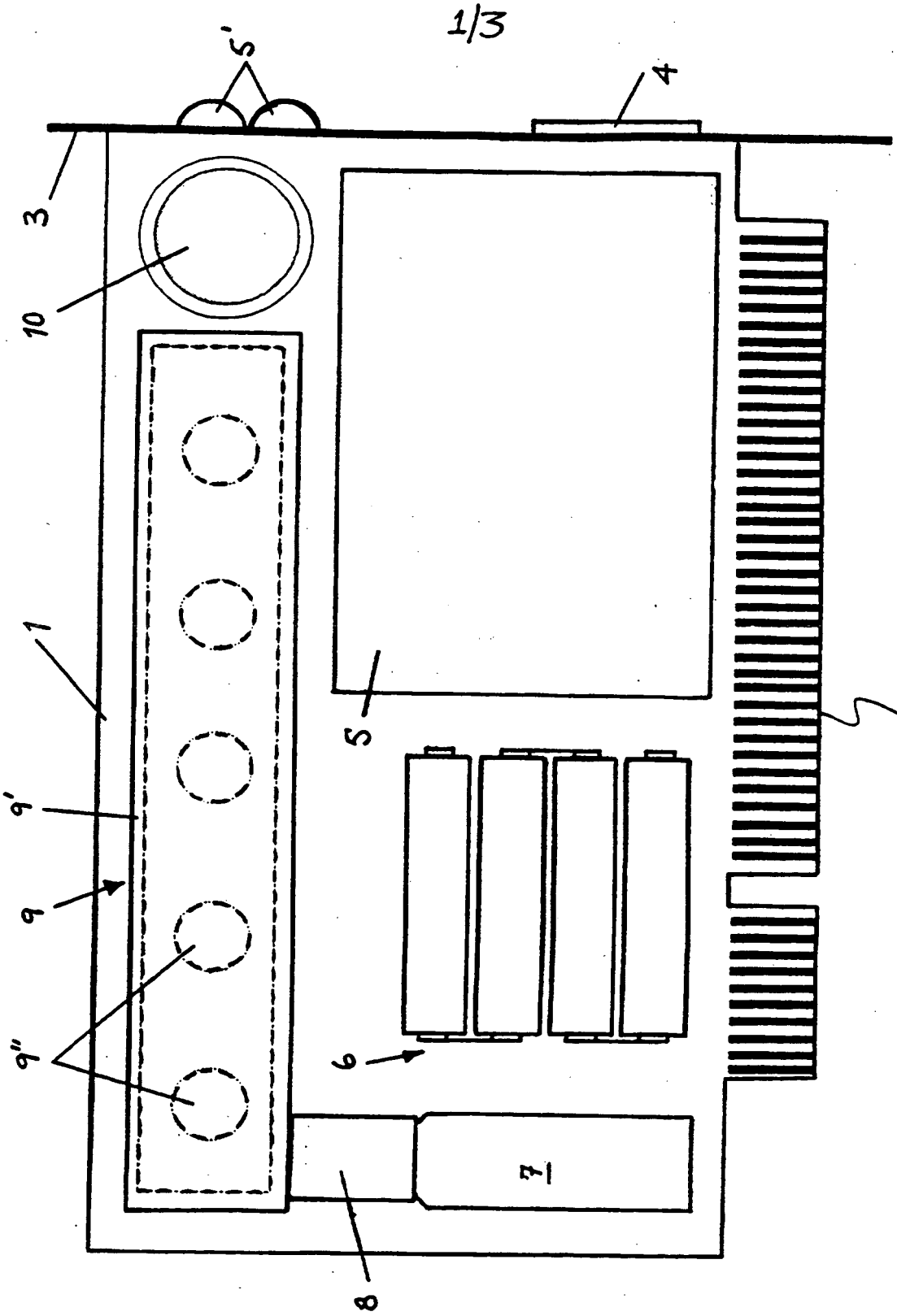

FIGURE 1

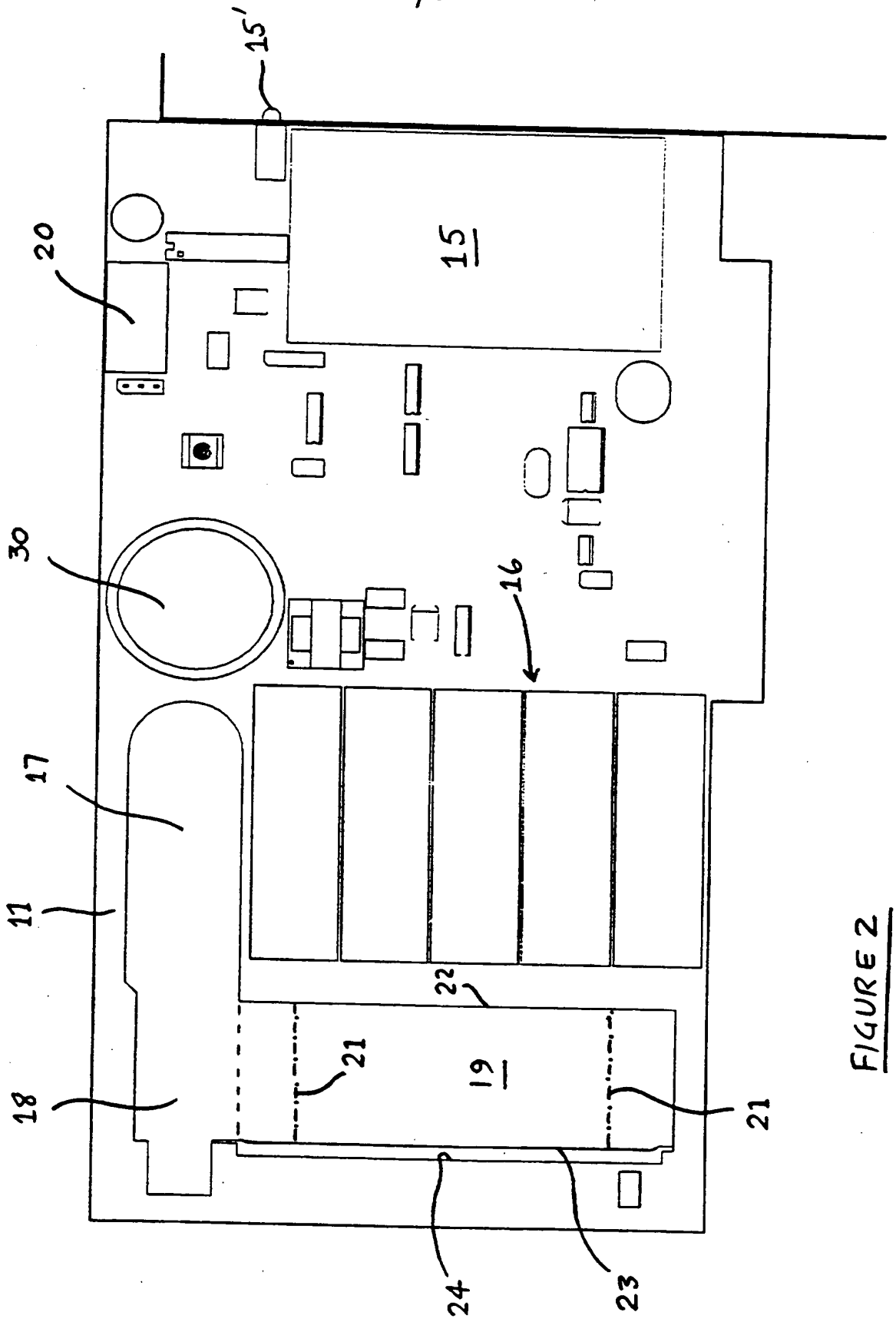

FIGURE 2

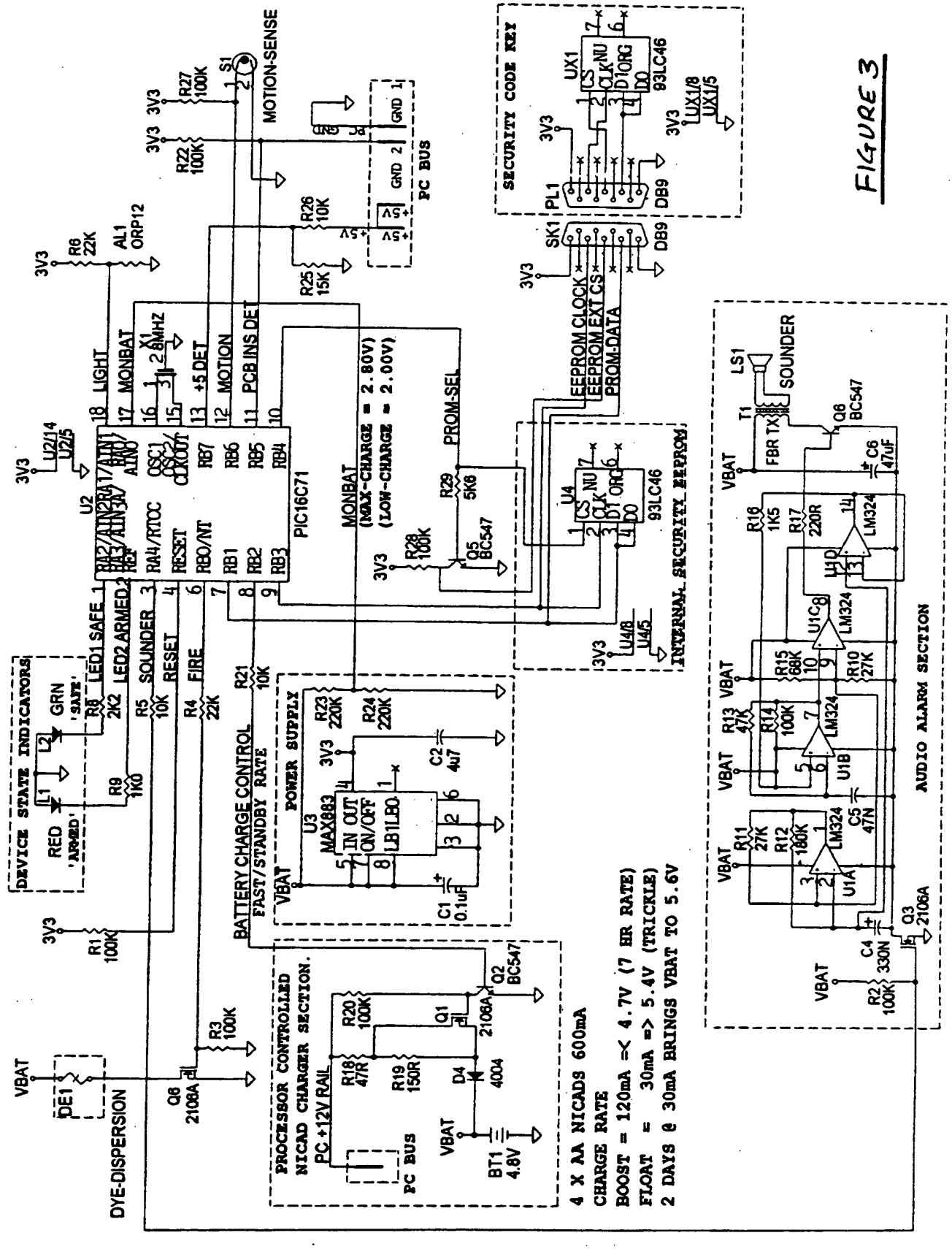

FIGURE 3

2303173

SECURITY DEVICE

The present invention relates to a security device for electrical or electronic equipment, especially, but not exclusively, for electronic computer equipment. The security device of the present invention has been developed particularly for use with small computers such as those known as PCs, micro computers or desktop computers.

PCs are a popular target for theft and are stolen in ever-increasing quantities. The level of security placed on a building in which PCs are housed does not appear to deter the PC thief and there is a ready market for stolen systems due to the high profit margins offered thereby and competitive nature of the computer industry.

There are many PC anti-theft devices on the market. These include, for example, chains for securing the PC to the desk and internal sounders intended to emit an audible alarm. Chains may readily be cut with bolt cutters and serve only to delay the theft. Internal sounders rarely seem to be taken seriously, and often are ignored.

There are two main types of PC theft which have to be contended with. One is the theft of the entire PC, possibly excluding the monitor as this is a bulky and low value item. The second is removal of internal high value parts only from within the PC casing. Such parts include, for example, the processor chips and memory modules. For a security device for PCs to work satisfactorily and gain widespread acceptance, it must give adequate protection against both these types of

theft.

There is no totally secure method or unbeatable system available for protecting PCs against such theft, bearing in mind that the PC is to be used in an environment where people normally have access to it. However, the security device of the present invention has for its object to overcome the disadvantages and shortcomings of prior art anti-theft devices and to confer effective and reliable protection to an item of electrical or electronic equipment, for example a PC or other type of computer equipment, in which the security device is installed.

A first aspect of the invention provides a security device for electrical or electronic equipment, comprising a sealed unit containing a supply of a marker substance, monitoring means arranged to detect any deviation from normal use or condition of electrical or electronic equipment with which the security device is associated in use, and means arranged to initiate release of the marker substance from the sealed unit into the equipment upon detection of any deviation of the equipment from normal use or condition thereof by said monitoring means.

Preferably, the sealed unit is rupturable by said initiating means upon detection by said monitoring means of any deviation of the equipment from normal use or condition thereof, to release marker substance from the unit into the equipment.

The sealed unit may comprise at least one line of weakness which is frangible by said initiating means

to effect rupture of the unit upon detection by said monitoring means of any deviation of the equipment from a normal use or condition thereof, to release marker substance from the unit into the equipment.

The at least one line of weakness may have at least a portion thereof arranged to lie in confronting, generally parallel relationship with respect to an edge of another component of the device or a component of the electrical or electronic equipment with which the security device is associated in use, such that, in use of the device and upon detection by said monitoring means of any deviation of the equipment from normal use or condition thereof and consequential breakage of said at least one line of weakness by said initiating means, at least some of the marker substance released from the ruptured unit impinges upon the edge of the component of the equipment, to generate an atomised spray of the marker substance within the equipment.

The monitoring means may comprise a motion or vibration detector, a light detector or any combination thereof.

Additionally or alternative, the monitoring means may comprise a transmitter/receiver pair which is arranged to determine its spatial relationship with respect to a component of electrical or electronic equipment with which the security device is associated in use and which, upon detection of a change in said relationship as a consequence of any deviation of the equipment from normal use or condition thereof, causes said initiating means to effect release of the marker substance from the sealed unit.

Preferably, the transmitter/receiver pair comprises an infra red transmitter and a receiver pair, such as a pair of light emitting diodes.

Alternatively, the transmitter/receiver pair comprises an ultrasonic transmitter and receiver pair.

In a further embodiment, the monitoring means comprises a tamper detector.

The security device is preferably arranged to operate continuously and irrespective of whether the equipment with which it is associated in use, is switched on or off and the monitoring means may comprise a microcontroller or microprocessor, preferably operable independently of the electrical or electronic equipment with which the device is associated.

A second aspect the present invention provides a security device for electrical or electronic equipment, the security device comprising a sealed unit containing a supply of a marker substance, and one or more detectors for monitoring the equipment and, upon detection of any deviation(s) from normal use or conditions of the equipment, operable to initiate release of the marker substance from the sealed unit.

In a third aspect of the present invention there is provided a security device for electrical or electronic equipment, the security device comprising a sealed unit containing a supply of a marker substance, and one or more detectors for monitoring the equipment and, upon detection of any deviation(s)

from normal use or conditions of the equipment, operable to initiate rupture of the sealed unit for release of the marker substance therefrom.

A fourth aspect the present invention provides, in combination, electrical or electronic equipment and a security device in accordance with any aspect of the invention, or modifications thereof, defined above.

A fifth aspect of the invention provides the combination of electrical or electronic equipment with a security device which is mounted and enclosed within a casing of the electrical or electronic equipment and comprises a sealed unit containing a supply of a marker substance, and one or more detectors for monitoring the equipment and, upon detection of any deviation(s) from normal use or conditions of the equipment, operable to initiate release of the marker substance from the sealed unit.

In another, sixth aspect of the present invention, there is provided electronic computer equipment comprising a casing enclosing at least a microprocessor and further substantially enclosing a security device comprising a sealed unit containing a supply of a marker substance, and one or more detectors for monitoring the equipment and, upon detection of any deviation(s) from normal use or conditions of the equipment, operable to initiate release of the marker substance from the sealed unit so that such substance may mark at least the microprocessor. Preferably the casing also encloses a memory module which may be marked with any marker substance when released.

Yet another aspect of the invention provides a method of protecting electrical or electronic equipment against unauthorised use, tampering or theft in accordance with yet another, seventh aspect of the invention comprises installing within a casing of the equipment a sealed unit containing a supply of a marker substance and monitoring, by means of one or more detectors, use and/or conditions appertaining to the equipment and, upon detection of any deviation(s) from normal use or conditions of the equipment, initiating release of the marker substance from the sealed unit.

As described above, a security device in accordance with the present invention preferably includes a motion detector which, when the security device is installed in the electrical or electronic equipment, for example computer equipment, to be protected and properly armed, will monitor the equipment for any movement. It will detect any motion such as would occur if an attempt were to be made to steal the equipment. Preferably, the motion detector or its associated electronics will ignore any movement of the equipment during its normal functioning, such as when the computer equipment is switched on and in use. At other times, when the computer equipment is switched off, should any motion or vibration of the equipment be detected by the motion detector an alarm state may be entered.

A security device in accordance with the present invention may also include a light detector which, when the security device is installed in the electrical or electronic equipment, for example computer equipment, to be protected and properly

armed, will monitor the equipment for any sudden change in light level. It will detect any sudden change in light level within the casing and enter an alarm in response thereto. The light detector is preferably arranged to function in this manner continuously and irrespective of whether the equipment is switched off or on.

A security device in accordance with the present invention may comprise a tamper detector which, when the security device is installed in the electrical or electronic equipment, for example computer equipment, to be protected and properly armed, will monitor the equipment for any attempt to disconnect or remove the security device itself or a component part thereof. It will detect any attempt to disconnect the security device, or component part thereof, from an operative connection with the electrical or electronic equipment, for example computer equipment, and enter an alarm condition in response thereto. This tamper detector is preferably arranged to function in this manner continuously and irrespective of whether the equipment is switched off or on.

Preferably, a security device in accordance with the present invention includes all three of the foregoing detectors.

The concept behind the security device of the present invention is that of devaluing the electrical or electronic equipment, for example computer equipment, or any of its especially valuable component parts, should any attempt be made to interfere with such equipment or remove it from its position of normal use. By devaluing the equipment or any of its

major, valuable parts, it will be not worth stealing. In operation of the security device in accordance with the present invention, the equipment in which it is installed is devalued by covering substantially all valuable internal component parts within the casing of the equipment with the marker substance, when the equipment is moved or interfered with in any unauthorised manner. This substance is preferably indelible, for example a dye. The released dye may also leak through, and out of, the casing to become visible on the outside. By devaluing the equipment, or its most valuable component parts, in this way it will become less readily saleable through dealers or to potential purchasers.

Preferably, the sealed unit containing the supply of the marker substance is rupturable in order to release the substance.

Preferably also, a security device in accordance with the present invention is constructed and adapted to be installed by a user and, in the case of its installation within a PC casing, will take up one expansion slot within the casing of that PC. Once installed, the security device preferably has to be armed by the use of an authorised software key.

The security device of the present invention may be based on the use of a microcontroller. In operation, this continuously monitors the device's environment and is arranged to sense sudden changes therein. The microcontroller is preferably totally independent, in operation, of the electrical or electronic equipment, for example, computer equipment, in which it is installed and receives power normally

from its own batteries. These may be rechargeable from the equipment, for example under microprocessor control, when the equipment, for example computer equipment, is in normal operation. Preferably, the software key for arming the unit is an electronic device with a 64-bit code, which plugs into an interface of the security device for arming and disarming the latter, and is removed at all other times.

Embodiments of the present invention will now be described in further detail by way of example and with reference to the accompanying diagrammatic drawings in which:

Figure 1 is a diagrammatic plan view of a first embodiment of security device;

Figure 2 is a diagrammatic plan view of a second embodiment of security device; and

Figure 3 is an electronic circuit diagram for use in the first embodiment of security device shown in Figure 1.

The security device of the present invention is intended for use with, and installation within the casing of, electrical or electronic equipment which is to be protected against unauthorised or abnormal movement, or tampering, such as by attempts to open the casing or disable or remove the security device itself or any components thereof. Whilst the security device in accordance with the present invention is generally applicable to the protection of any desired electrical or electronic equipment, it is particularly

intended to be installed within the casing of computer equipment, such as a desktop computer or PC. Accordingly, in the description which follows, embodiments of security device in accordance with the present invention are described as constructed and adapted for installation within the casing of computer equipment. However, it will be apparent to those skilled in the art that adaptations to other items of electrical or electronic equipment may be made without exercise of inventive ingenuity and within the scope of the present invention as most broadly defined in this specification.

Figure 1 of the drawings shows in diagrammatic plan view a board constructed and dimensioned for insertion within an expansion slot normally available within the external casing of a microcomputer.

This first embodiment of security device comprises a board 1, as is well known in the art, having a lower edge connector 2 affording electrical contacts which, upon insertion of the lower edge of the board 1 within the desired expansion slot (not shown) within the computer casing, will make electrical connection with appropriate terminals of the expansion slot.

One end edge of the board 1 has a mounting plate 3, normally a metallic plate, which will be received within an opening at the rear of the computer casing and by which the entire board will be securely fixed and held in position to the computer casing. On one side of the plate 3 opposite that from which the board 1 projects, is a plug-type interface 4 for the releasable connection of a software key, and a pair of

indicators 5', for example a green and a red LED, which will, in operation of the security device, give visible indications of its operational state. When the board 1 and plate 3 are properly installed within an expansion slot within the casing of the computer, the interface 4 for the software key and the indicators 5' will be exposed at the rear exterior of the computer where they may be seen or accessed as required.

Mounted on the board 1 is an electronic module 5, a rechargeable battery pack 6, a container 7 of CO_2 gas, a gas motor 8, a sealed dye unit 9 containing, preferably indelible, marker substance or dye, and an audible alarm sounder 10.

The electronic module 5 comprises, inter alia, three detectors, namely a motion detector, a light detector, and a tamper detector (not shown).

The motion detector is intended to detect any unauthorised or abnormal movement and so, when the security device is installed within the casing of a computer and appropriately armed using a software key, any unexpected or sudden movement of the casing will be sensed. However, in order to obviate false alarms, the motion detector, or its associated electronics of the electronic package, is arranged not to respond to any abnormal movements when the computer is switched on. This allows for general vibration, or even accidental events such as falling from the desktop, during normal every day use of the computer.

On the other hand, when the computer is switched off the motion detector will be sensitive to any

vibration of the casing and, upon detection of such vibration or other movement, cause a loud intermittent sound to be emitted from the audible sounder 10. If the detected movement is continuing and constant, the emitted sound will become more persistent with time. This ensures that any accidental movement, for example by an authorised person such as an office cleaner, may be taken into account. This first phase of alarm may be timed to last for only a short predetermined time period, for example 1 minute. If, during this period the vibration or movement has been protracted or violent then the second phase of alarm will be entered. However, under all other conditions including at the end of this first period, the casing is not subjected to further vibration or movement, then the audible sounder 10 will fall silent. And, in the absence of further vibration or movement during the first period and after the initial disturbance, the audible sounder will gradually decrease its sound output level. However, if the motion detector senses any further vibration or movement at the end of the predetermined period of the first phase of alarm, a second phase of alarm will be entered.

During the second phase of alarm the sound emitted from the audible sounder 10 will be continuous and at a high level. If, during this phase no further movement is detected, the alarm state will eventually cease and the security device will resume its normal monitoring by way of the motion detector. If, however, during this second phase any further vibration or movement is detected by the motion detector, action will be initiated to cause release of dye from the sealed dye unit 9.

The light detector is intended to prevent unauthorised entry to the interior of the computer casing, such as might be attempted in order to remove the microprocessor or memory modules or other valuable components enclosed therewithin. Normally, with the security device appropriately installed and all reasonable steps having been taken to seal the computer casing against ingress of light, the interior of the casing will be quite dark. Should an attempt be made to remove a portion of the casing, there will be a sudden change of light level therewithin. Thus, even if the intruder is sufficiently careful about removing the casing portion and succeeds in doing so without triggering the motion detector, the light detector will, nevertheless, respond to the intrusion. Should there be detected any sudden change in light level within the casing, as sensed by the light detector, action will again be taken to initiate release of the dye from the normally sealed dye unit 9. The amount of light normally present within the computer casing will vary from computer casing to computer casing and there will also be some interference from external light sources, such as the sun. In order to compensate for such variations and external influences, the light detector and its associated electronics within the electronics package 5 is arranged to continuously monitor gradually changing light conditions within the casing and periodically to adjust its threshold detection level accordingly.

The tamper detector is constructed and arranged to continuously monitor circuit continuity across a selected pair of the edge connector contacts of the board 1. Thus, should any attempt be made to unplug

and remove the board 1 from the expansion slot within the computer casing, loss of circuit continuity will be sensed by the tamper detector and action will be initiated to cause release of dye from the normally sealed dye unit 9.

The electronics module 5 includes a PIC integrated circuit chip which, in operation, inter alia converts analogue signals to digital signals within the chip, so minimising the need for other electronic components outside the chip. Upon arming of the security device and under control of this PIC chip, initial checks are carried out in order to validate the status of the security device. Such initial checks include, for example, a check to determine whether the board 1 is properly plugged into the expansion slot within the computer casing, that the computer casing is not in a state of vibration or other movement, and that the light dependent resistor (LDR), which preferably forms the sensitive component of the light detector, is operating in an acceptably satisfactory environment having regard to the light sensitivity requirements of the light detector. For example, if, upon installation of the security device within the computer casing, openings within the rear of the casing have not been closed off, the initial light level within the casing will be excessive and the security device will not arm. Visible warning of this condition will be given by continuous flashing of both the green and red LEDs 5' exposed to view on the mounting plate 3 of the security device.

The electronics module 5 affords a "watchdog" timer based on a free running oscillator. In order to conserve electrical power, supplied from the

rechargeable battery pack 6 when the computer in which the security device is installed, is switched off, the main electronics circuitry enters a "sleep" mode from which it is "wakened" periodically, for example every 2.3 seconds, for checks to be run. These checks embrace, for example, the light level within the computer casing, and voltage of the rechargeable battery pack 6. Should any problem occur, for example a software crash or overload, the "watchdog" timer will not be correctly acknowledged and an immediate reset will be initiated. This involves complete re-arming of the security device from scratch, including running all the usual checks, and should any problem be detected, the LEDs 5' will flash. The security device is, thus, completely self-monitoring both when the computer is off and on. Provided the "watchdog" timer is correctly acknowledged, it will return the main electronics circuitry to its "sleep" mode.

Should any of the detectors sense any unauthorised of abnormal disturbance, such as motion of the casing, a sudden increase in light level within the casing, or an attempt to unplug the board 1, the main electronics circuitry will immediately be "awakened" from its "sleep" mode so that the alarm may be entered, if appropriate. The light and tamper detectors operate continuously, whether the computer is switched off or on, and will initiate an alarm state should either of them sense any unauthorised or abnormal condition related to their functions. However, the motion detector does not respond to vibration or other movement of the computer casing whilst the computer is switched on, though normal flashing of the LEDs 5' periodically, each time the unit is "awakened" from its "sleep" mode will,

nevertheless, occur. The motion detector is preferably disarmed by switching on electrical power to the computer. The rechargeable battery pack 6 is maintained in an appropriately charged state by drawing power from the computer when the latter is switched on.

If, at any time, one or more of the detectors senses an unauthorised or abnormal disturbance of the computer and an alarm state is entered, electrical current is fed to the gas motor 8 in order to heat a resistive wire element therein. The wire element is embedded within a reactive chemical which, when heated, will rapidly release a large volume of gas which will drive a pin to rupture the carbon dioxide container 7. Release of CO_2 from the carbon dioxide container 7 causes an aluminium foil seal at an entry point of the dye container 9 to be ruptured, whereby carbon dioxide rapidly enters the dye container 9 and pressurises the same. The rapid rise of pressure within the dye container 9 causes an aluminium foil seal 9' over its dye outlet ports 9'' to be blown away and, under the continuing influence of the carbon dioxide gas, the dye is projected within the computer casing so that it may cover all components therein, for example the microprocessor and memory modules and any other particularly valuable components. The dye may also leak from within the computer casing to give visible external indication that the security device has been triggered.

Initial installation and operation of the security device proceeds as follows.

Assuming a computer to be protected by the

security device has previously been unused and has just had the security device installed therewithin as described above, it will be apparent to those skilled in the art that, to date, the computer will not have generated a unique 64-bit number related specifically to it.

A user of the computer, with the security device installed, is required to plug in at the interface 4 a software key. This software key may come in either one of two forms, namely, a "corporate key" and a "single-user key". The relevant software key is plugged in at the interface 4 and the computer initially booted up in well known manner. Because this is the first use of the computer, a unique 64-bit number will be generated thereby and stored in an EEPROM, as is known. This 64-bit number will also be supplied to the software key plugged in at the interface 4 and similarly stored therein in an EEPROM. If the software key plugged in at the interface 4 is a "corporate key" then this key additionally incorporates an unique corporate code which enables the key subsequently to be used on any other computers within the same organisation, and thus functions as a master key. However, if the software key plugged in at the interface 4 is a "single-user key", it omits any such corporate code and thus may be used only with one and the same computer.

In order to provide the facility for replacement software keys, for example should there be loss or accidents to existing keys, replacement software keys will be provided and suitably encoded for recognition by a previously-used computer. Once recognised, the replacement software key will receive from the

computer its unique 64-bit number previously generated and stored therein, and a code previously contained within the replacement software key and which indicated its replacement status will be cleared.

A second embodiment of security device shown in Figure 2 operates in substantially the same manner as the first embodiment of security device described above in relation to Figure 1, except that it comprises to modifications over that first embodiment.

Firstly, the second embodiment of security device comprises a spatial monitoring unit 20 which comprises a pair of light emitting diodes (also not shown), one being a transmitter and the other, a receiver for reflected infra red radiation from the transmitter. This LED transmitter/receiver pair is arranged to determine its spatial relationship with respect to a component, such as a portion of the casing, of the computer in which the security device is installed. Upon detection of a change in that spatial relationship, such as, the removal or attempted removal of, say, the casing portion of the computer, then dye contained in the otherwise sealed unit 19 is released to stain components of the computer.

The second modification relates to the manner in which the dye contained in the sealed unit 19 is released therefrom and is distributed to components of the computer.

The generally square cross-sectioned housing of the sealed unit 19 has lines of weakness of which only two are shown at 21 in chain-dotted lines. Another of these lines of weakness, which acts as a hinge,

extends along the interior of the rear wall 22 of the housing of the unit 19 between the lines of weakness 21, whilst a further line of weakness extends along the front wall 23 of the housing of the unit 19 again between the lines of weakness 21.

The line of weakness 22 is in confronting parallel relationship with an edge 24 of the board 11 of the security device such that, in an alarm condition of the device where release of the dye from the normally sealed unit is effected by rupture of the lines of weakness 21 and that extending along the front wall 23 of the unit housing, dye impinges upon the board edge 24 at high velocity, due to the pressure of the gas (CO_2) exhausting from the container 17 into the unit 19, to generate an atomised spray of the dye within the computer, thereby enhancing distribution of the dye therewithin.

Otherwise, the other components of this second embodiment of security device are generally the same as those of the first embodiment of security device, namely, the electronic module 15, the rechargeable battery pack 16, the gas motor 18 or other suitable gas release device, and the audible alarm sounder 30.

Should a computer with the security device installed therein be left unused for a considerable period of time, for example three or more months, the voltage of the rechargeable battery pack 6, 16 may decline to below the level necessary to sustain normal functioning of the security device. The device thus monitors the battery voltage and, upon detection of any such low voltage condition, the security device disarms itself. However, in order not to give undue

warning of this state, and thus provide a potential thief or intruder with information enabling him to intrude upon or steal the computer while subjecting himself to low risk of detection, the LEDs 5', 15' will continue to flash as normal until the battery voltage falls to a level at which this, too, becomes impossible.

A diagram of a typical circuit of the electronic module 5 used in the first embodiment of security device described above, is shown in Figure 3.

The security device of the present invention is easy and convenient to install within a computer casing and offers safe and reliable functioning whilst affording secure protection of the computer, or its major components, in whose casing the device is installed. The security device of the present invention enables the computer to be used in normal conditions and by any authorised user without subjecting such user to any inconvenience. However, should the computer be subjected to any abnormal or unauthorised actions, whether by an authorised user or potential thief or intruder, the security device of the present invention will raise an alarm and, if appropriate, cause release of the, preferably indelible, marker substance or dye which will spread over at least the main internal and most valuable components of the computer, rendering them virtually unsaleable. The marker substance or dye chosen will be non-toxic to human beings, so that should any person become contaminated thereby he or she will not be subjected to any health risks.

The security device of the present invention is

not limited to the particular details of the currently preferred embodiment as described hereinabove, but embraces all such variations as fall within the scope of the broadest statement of the invention contained herein.

CLAIMS

1. A security device for electrical or electronic equipment, comprising a sealed unit containing a supply of a marker substance, monitoring means arranged to detect any deviation from normal use or condition of electrical or electronic equipment with which the security device is associated in use, and means arranged to initiate release of the marker substance from the sealed unit into the equipment upon detection of any deviation of the equipment from normal use or condition thereof by said monitoring means.

2. A security device according to claim 1, wherein the sealed unit is rupturable by said initiating means upon detection by said monitoring means of any deviation of the equipment from normal use or condition thereof, to release marker substance from the unit into the equipment.

3. A security device according to claim 2, wherein the sealed unit comprises at least one line of weakness which is frangible by said initiating means to effect rupture of the unit upon detection by said monitoring means of any deviation of the equipment from normal use or condition thereof, to release marker substance from the unit into the equipment.

4. A security device according to claim 3, wherein said at least one line of weakness has at least a portion thereof arranged to lie in confronting, generally parallel relationship with respect to an edge of a component of the electrical or electronic equipment with which the security device is associated

in use, such that, in use of the device and upon detection by said monitoring means of any deviation of the equipment from normal use or condition thereof and consequential breakage of said at least one line of weakness by said initiating means, at least some of the marker substance released from the ruptured unit impinges upon the edge of the component of the equipment, to generate an atomised spray of the marker substance within the equipment.

5. A security device according to any preceding claim, wherein said monitoring means comprises a motion or vibration detector.

6. A security device according to any preceding claim, wherein said monitoring means comprises a light detector.

7. A security device according to any preceding claim, wherein said monitoring means comprises a transmitter/receiver pair which is arranged to determine its spatial relationship with respect to a component of electrical or electronic equipment with which the security device is associated in use and which, upon detection of a change in said relationship as a consequence of any deviation of the equipment from a normal use or condition thereof, causes said initiating means to effect release of the marker substance from the sealed unit.

8. A security device according to claim 7, wherein the transmitter/receiver pair comprises an infra red transmitter and a receiver pair.

9. A security device according to claim 8, wherein

the infra red transmitter and receiver pair comprises a pair of light emitting diodes.

10. A security device according to claim 7, wherein the transmitter/receiver pair comprises an ultrasonic transmitter and receiver pair.

11. A security device according to any preceding claim, wherein said monitoring means comprises a tamper detector.

12. A security device according to any preceding claim arranged to operate continuously and irrespective of whether the equipment with which it is associated in use, is switch ed on or off.

13. A security device according to any preceding claim, wherein said monitoring means comprises a microcontroller or microprocessor.

14. A security device according to claim 13, wherein the microcontroller or microprocessor is operable independently of the electrical or electronic equipment with which the device is associated in use.

15. A security device for electrical or electronic equipment, the security device comprising a sealed unit containing a supply of a marker substance, and one or more detectors arranged to monitor the equipment and, upon detection of any deviation(s) from normal use or conditions of the equipment, to operate to initiate release of the marker substance from the sealed unit.

16. A security device for electrical or electronic

equipment, the security device comprising a sealed unit containing a supply of a marker substance, and one or more detectors arranged to monitor the equipment and, upon detection of any deviation(s) from normal use or conditions of the equipment, to operate to initiate rupture of the sealed unit to release marker substance therefrom.

17. In combination, electrical or electronic equipment and a security device according to any preceding claim.

18. The combination of electrical or electronic equipment and a security device which is mounted and enclosed substantially within a casing of the electrical or electronic equipment and which comprises a sealed unit containing a supply of a marker substance, and one or more detectors arranged to monitor the equipment and, upon detection of any deviation(s) from normal use or conditions of the equipment, to operate to initiate release of the marker substance from the sealed unit.

19. Electronic computer equipment comprising a casing enclosing at least a microprocessor and a security device which comprises a sealed unit containing a supply of a marker substance and one or more detectors arranged to monitor the equipment and, upon detection of any deviation(s) from normal use or conditions of the equipment, to operate to initiate release of the marker substance from the sealed unit so that such substance marks at least the microprocessor.

20. Equipment according to claim 19, wherein the casing also encloses a memory module which can be

marked with marker substance when so released.

21. A security device or equipment, as the case may be, in accordance with any preceding claim, wherein the marker substance is a dye, preferably indelible.

22. A method of protecting electrical or electronic equipment against unauthorised use, tampering or theft, comprising installing within a casing of the equipment a sealed unit containing a supply of a marker substance and monitoring, by means of one or more detectors, use and/or conditions relating to the equipment and, upon detection of any deviation(s) from normal use or conditions of the equipment, initiating release of the marker substance from the sealed unit.

23. A security device substantially as hereinbefore described with reference to the accompanying drawings.

The Patent Office

27

Application No: GB 9614616.2
Claims searched: 1 - 23

Examiner: Justin Black
Date of search: 11 October 1996

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.O): E2X

Int Cl (Ed.6): G08B (15/02). E05G (1/14).

Other: On-line: WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
Y	GB 2280056 A	(TRANSALARM). Page 3 lines 1 - 2 and page 4 lines 14 - 18.	5, 11
Y	GB 2269205 A	(TOTAL SECURITY). Page 10 lines 9 - 12 and 22 - 24, and page 4 lines 28 - 31.	5, 13
X, Y	EP 0196944 A1	(SONIS). See abstract.	X: 1, 15, 16, 18, 22 Y: 2, 3, 4, 5, 6, 11, 13, 19, 21
Y	EPO347091	(TRANSALARM). Column 3 lines 28 - 33 and column 4 lines 20 - 27.	5, 6
Y	WO 80/00887	(INNOVATIONSTEKNIK). See page 6 lines 17 - 23, page 12 lines 4 - 5 and 11 - 12.	2, 3, 4, 13, 21
Y	US 4908608	(REINKE). See abstract and column 3 line 11 - 14.	5, 19

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.